



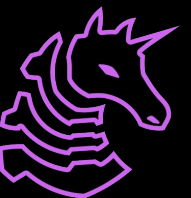
FA2024 Week 06 • 2024-10-10

# Hardening Windows Default Installations & Process Isolation

Sagnik Chakraborty, Michael Khalaf

# Baseline: Group Policy Objects (GPOs)

1. Password Complexity (12+ characters, numbers, + special characters) to evade password cracks.
2. Account lockout thresholds
3. Secure logon
4. Kill unnecessary processes, applications, and limit services
5. Practice least privilege for organizations.
  - a. Forests, Groups, AD group segmentations.



# GPO Hardening

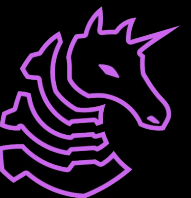
1. Passwords: set a minimum age, length, and character/number/special char composition.
2. Disable SMBv1/2/3 and more unless needed.
  - > Mitigation: lateral movement via credentials & protocols.
  - > Suggestion: Microsoft Security Compliance Toolkit



# Credential Guards & LSA Protection

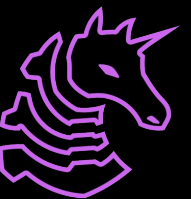
- > Enable **Credential Guard** using domestics like Group Policy and Intune
  - > Virtualize and isolate LSASS
- > LSA Protection enabled = restrict LSASS access

**Mitigation:** Restrict access to LSASS & prevent memory scraping for credentials. Restrict tools like Mimikatz (etc)



# WDAC & ASR

- > Configure **WDAC** policy to accept trusted software & relevant drivers (printers!)
- > Implement ASR Rules
  - >



# Next Meetings

**2024-10-15 • Next Tuesday**

-

**2024-10-17 • Next Thursday**

-

